

BEST AVAILABLE COPY

JP00/6355

PCT/JP00/06355

28.09 99

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D 13 OCT 2000

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

22/3

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

1999年 9月16日

ESU

出 願 番 号

Application Number:

平成11年特許願第262766号

出 願 人

Applicant(s):

松下電器産業株式会社

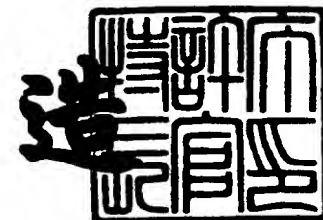
PRIORITY  
DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 9月18日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3075476

【書類名】 特許願  
 【整理番号】 2030714027  
 【提出日】 平成11年 9月16日  
 【あて先】 特許庁長官殿  
 【国際特許分類】 H04M 15/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地  
 松下電器産業株式会社内

【氏名】 高山 久

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地  
 松下電器産業株式会社内

【氏名】 松瀬 哲朗

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地  
 松下電器産業株式会社内

【氏名】 川口 京子

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地  
 松下電器産業株式会社内

【氏名】 中西 良明

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地  
 松下電器産業株式会社内

【氏名】 佐々木 理

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

特平 1 1 - 2 6 2 7 6 6

【代理人】

【識別番号】 100082692

【弁理士】

【氏名又は名称】 蔵合 正博

【電話番号】 03(3519)2611

【手数料の表示】

【予納台帳番号】 013549

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9004843

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子財布

【特許請求の範囲】

【請求項 1】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 2】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 1 記載の電子財布。

【請求項 3】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 4】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 3 記載の電子財布。

【請求項 5】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 6】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 5 記載の電子財布。

【請求項 7】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 8】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 7 記載の電子財布。

【請求項 9】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 10】 前記電子情報から電子情報オブジェクトを生成し前記電子情

報を制御する手段を備えた請求項 9 記載の電子財布。

【請求項 1 1】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 1 2】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 1 1 記載の電子財布。

【請求項 1 3】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 1 4】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 1 3 記載の電子財布。

【請求項 1 5】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 1 6】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 1 5 記載の電子財布。

【請求項 1 7】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 1 8】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 1 7 記載の電子財布。

【請求項 1 9】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 20】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 19 記載の電子財布。

【請求項 21】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示ソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 22】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 21 記載の電子財布。

【請求項 23】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 24】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 23 記載の電子財布。

【請求項 25】 少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示ソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項 26】 前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項 21 記載の電子財布。

【請求項 27】 前記電子情報を構成する前記サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せであることを特徴とする請求項 23 から請求項 26 記載の電子財布。

【請求項 28】 前記電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、前記サービス制御情報に基づく決済データを重畳することを特徴とする請求項 23 から請求項 26 記載の電子財布。

【請求項 29】 前記電子情報の電子情報オブジェクトが、決済処理時に交換

する各メッセージに、前記サービス制御モジュール情報の組合せに基づく決済データを重畳することを特徴とする請求項 27 記載の電子財布。

【請求項 30】 前記電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであることを特徴とする請求項 28 または請求項 29 記載の電子財布。

【請求項 31】 前記電子情報の表示手段を備えることを特徴とする請求項 1 から請求項 30 記載の電子財布。

【請求項 32】 前記電子情報から表示情報を生成する手段を備えることを特徴とする請求項 1 から請求項 30 記載の電子財布。

【請求項 33】 請求項 1 から請求項 32 に記載の前記電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記録媒体。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、プリペイドカードやクレジットカード（バンクカード）に代表される小売販売取引における決済機能、各種イベント、公演、映画等のチケットの改札機能、さらには、それら、プリペイドカードやチケットの流通・販売機能を提供するエレクトロニックコマースシステムに関し、特に、利便性と、決済の安全性を担保し、効率的で、円滑な商取引を可能にするものである。

##### 【0002】

##### 【従来の技術】

近年、電子マネーや電子チケットなど価値情報を電子化し、流通を効率化しようとする取り組みが行われている。

その一つの方式として、その価値情報が持つ属性をマークアップ記述言語で規定して、それに所有者のデジタル署名を施すことによって、流通を可能にする方式がある。図 21（a）は、従来の技術における価値情報の発行者のセンターサー

バ 2 1 0 0 からユーザの I C カード 2 1 0 1 に、電子化された価値情報 2 1 0 3 が発行された状態を示す模式図である。I C カード 2 1 0 0 に格納された価値情報 2 1 0 3 は、マークアップ記述言語によって、価値情報が持つ属性が記述されており、不正な改竄を防止するため、全体に対して発行者(Issuer)によるデジタル署名が施されている。また、図 2 1 (b) は、従来の技術における電子化された価値情報 2 1 0 3 がマーチャントに対して使用された状態を示す模式図である。マーチャント端末 2 1 0 2 に格納されている価値情報 2 1 0 4 は、I C カード 2 1 0 0 に格納されていた価値情報 2 1 0 3 に、所有者の変更を示す情報を付加し、不正な改竄を防止するため、ユーザ(User)によるデジタル署名が施されたものである。情報は変更せず、追加するだけなので、改竄等の不正行為に対する安全性が高く、電子化された価値情報を安全に流通させることが出来る方式である。

【0 0 0 3】

【発明が解決しようとする課題】

しかしながら、従来の方式では、電子化された価値情報が流通する度に、電子化された価値情報のデータサイズが大きくなってしまい、取り扱いが不便であった。また、従来の方式では、電子化された価値情報を流通させる時に、双方の証明書を交換してデジタル署名を検証する必要があり、匿名性が確保できないという課題があった。さらに、従来の方式では、価値情報の種類により電子化の方式が異なり、例えば、プリペイドカードやチケットを統一的に取り扱うことができないという課題があった。

【0 0 0 4】

本発明は、こうした従来の技術の課題を解決するもので、匿名性と安全性、および利便性に優れ、価値情報の効率的な電子化と、各種の電子化された価値情報をユーザが効率的に取り扱うことが出来る電子財布を提供することを目的としている。

【0 0 0 5】

【課題を解決するための手段】

これらの課題を解決するために本発明は、第 1 に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報とを備えた電子情報を、保存管理す



る手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【 0 0 0 6 】

第 2 に、第 1 の電子財布に、電子情報から電子情報オブジェクトを生成し電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【 0 0 0 7 】

第 3 に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【 0 0 0 8 】

第 4 に、第 3 の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【 0 0 0 9 】

第 5 に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

## 【 0 0 1 0 】

第 6 に、第 5 の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【 0 0 1 1 】

第 7 に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【 0 0 1 2 】

第8に、第7の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0013】

第9に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の可変の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【0014】

第10に、第9の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0015】

第11に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報に署名がされているので、発行者が規定した表示が保証される。

【0016】

第12に、第11の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0017】

第13に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を電子財布が備えたものである。表示制御情報の識別情報に署名がされているので、発行者が規定した表示が保証される。

【0018】

第14に、第13の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0019】

第15に、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示リソースの識別情報に署名がされているので、発行者が規定したイメージが保証される。

【0020】

第16に、第15の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0021】

第17に、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報の識別情報および表示リソースの識別情報に署名がされているので、発行者が規定した表示が保証される。

【0022】

第18に、第17の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0023】

第19に、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証

することができ、安全性が向上する。

【0024】

第20に、第19の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0025】

第21に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。

電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0026】

第22に、第21の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0027】

第23に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布を備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

【0028】

第24に、第23の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0029】

第25に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示

制御情報の識別情報と表示リソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

## 【0030】

第26に、第25の電子財布に、~~電子情報から電子情報オブジェクトを生成し~~前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0031】

第27に、サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せにしたものである。サービス制御モジュール情報の組合せを変更することにより、各種の電子情報を規定することが出来る。

## 【0032】

第28に、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御情報に基づく決済データを重畳するようにしたものがある。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

## 【0033】

第29に、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御モジュール情報の組合せに基づく決済データを重畳するようにしたものである。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

## 【0034】

第30に、電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

【0035】

第31に、電子情報の表示手段を備えるようにしたものであり、電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【0036】

第32に、電子情報から表示情報を生成する手段を備えるものであり、内容が変化した電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【0037】

第33に、請求項1から請求項32に記載の電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録したものであり、これにより、プログラムを、持ち運び可能な形態で、流通させることができる。

【0038】

【発明の実施の形態】

以下、本発明の実施の形態について、図1から図21を用いて説明する。なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その趣旨を逸脱しない範囲において、種々なる態様で実施し得る。本発明の具体的な実施形態の一つであるモバイル・エレクトロニックコマース・システムは、個人消費者が、ネットワークを介して、各種のチケットや、プリペイドカードを電子情報として購入し、チケットの改札や、一般の小売販売店で商品を購入の際に、係員に対してチケットを提示したり、店員との間で、直接、現金やレシートを受け渡したりすることなく、全て、無線通信によって、チケットの改札、商品やサービスの売買決済を行なうシステムである。

【0039】

以下では、本システムをモバイル・エレクトロニックコマース・システムと呼び、本システムで扱われる電子化されたチケットやプリペイドカードを電子バリュー、本システムによって提供される各種のサービスを、総称して、モバイル・エレクトロニックコマース・サービスと呼ぶこととする。このモバイル・エレクトロニックコマース・システムは、図1のシステム構成図に示すように、2系統の双方向無線通信機能とブラウザ機能と電子財布機能とを持つモバイルユーザ端末101と、双方向の通信機能とブラウザ機能と電子財布機能とを持つユーザ端

末107と、電子バリューの改札決済処理を行なうサービス端末105と、オンライン上で電子バリューの改札決済処理を行なうサービスサーバ106と、銀行、クレジットサービス会社または決済処理会社における口座決済処理を行なう決済処理サーバ104と、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う情報提供サーバ102と、電子バリューを生成・発行する電子バリュー発行サーバ103とを備え、これらはインターネット100によって結ばれている。サービスサーバ106と決済処理サーバ104と情報提供サーバ102と電子バリュー発行サーバ103とは、それぞれ、1台もしくは複数台のコンピュータによって構成されるシステムである。

#### 【0040】

モバイルユーザ端末101は、赤外線通信とデジタル無線通信との2系統の双方向無線通信機能と、ブラウザ機能と電子財布機能とを持つ携帯無線電話端末である。また、サービス端末105は、赤外線通信とデジタル無線通信との2系統の双方向無線通信機能を持ち、用途に応じて据置タイプや携帯タイプがある。なお、図1において、108と113は、モバイルユーザ端末101とサービス端末105が、それぞれ、インターネット100にアクセスしている際に行うデジタル無線通信の伝送路を示し、109は、モバイルユーザ端末101がサービス端末105と行う赤外線通信の伝送路を示し、110、111、112、114、115は、それぞれ、サービス提供サーバ102、電子バリュー発行サーバ103、決済処理サーバ104、サービスサーバ106、ユーザ端末107がインターネット100に接続するデジタル通信回線を示している。

#### 【0041】

モバイル・エレクトロニックコマース・サービスの通常の運用形態としては、次のような形態を想定している。決済処理サーバ104は、銀行またはクレジットカード会社または決済処理会社に設置され、情報提供サーバ102は、イベント会社、チケット発行会社、小売販売会社またはプリペイドカード発行会社に、情報提供サーバ102は、オンライン上で電子バリューに関する情報の提供および電子バリューの販売を行う事業会社にそれぞれ設置される。また、サービス端末105は、据置タイプの場合には、映画館やイベント会場等の入口、小売販売

店のレジカウンタに設置され、携帯タイプの場合には、売場販売員や、集金担当者が携帯し、サービスサーバ106は、オンラインショップやインターネット放送など電子バリューに応じたサービスを提供する会社に設置される。モバイルユーザ端末101は、消費者が持ち歩き、ユーザ端末107は、消費者が自宅に設置する。電子バリュー発行サーバ103は、モバイル・エレクトロニックコマース・サービスを提供する会社に設置される。さらに、モバイル・エレクトロニックコマース・システムを構成する各機器、および、各システムの所有者間の社会的な関係として、次のような関係を前提としている。

## 【0042】

モバイルユーザ端末101の所有する消費者は、銀行またはクレジットカード会社との間で、口座決済サービスの契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの会員契約を結んでいる。サービス端末105の所有者とサービスサーバ106の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、モバイル・エレクトロニックコマース・サービスの加盟店契約を結んでいる。但し、サービス端末105の所有者またはサービスサーバ106の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。情報提供サーバ106の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、情報提供サーバ106からの要求に応じて、電子バリュー発行サーバ103が電子バリューを発行する契約を結んでいる。但し、情報提供サーバ106の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。

## 【0043】

以下では、本システムの説明を簡単にするために、モバイルユーザ端末101の所有する消費者をユーザ(User)、サービス端末105またはサービスサーバ106を所有し、商品やサービスを提供・販売する事業者をマーチャント(Merchant)、電子バリュー発行サーバ103を所有しモバイル・エレクトロニックコマース・サービスを提供する会社をサービス提供者(Service Provider)、決済処理サーバ104を所有し口座決済処理を行なう銀行、クレジットカード会社または決



済処理会社を決済処理機関(Transaction Processor)、情報提供サーバ102を所有し、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う事業者を電子バリュー販売者(Electronic Value seller)呼ぶこととする。本システムによって提供されるモバイル・エレクトロニックコマース・サービスは、ネットワークを介したチケットやプリペイドカードの売買と、それに伴うそれらの配送と、それらチケットやプリペイドカードの使用を、全て電子的に行なうサービスである。具体的には、ユーザがモバイルユーザ端末101を用いて、インターネットを介して、情報提供サーバ102に電子バリューの購入オーダーをし、電子バリュー発行サーバ103から、情報提供サーバ10の電子バリュー発行要求に基づいて電子バリュー発行サーバ103が生成した電子バリューを受信して、それをモバイルユーザ端末101に蓄積して管理し、電子バリューを使用する際には、サービス端末105またはサービスサーバ106とのデータ通信によって、モバイルユーザ端末に蓄積されている電子バリューを提示し、電子バリューの改札決済処理情報を交換して、電子バリューの改札決済処理を行い、マーチャントが提供するサービスまたは商品の提供を行うものである。また、この時の電子バリューの売買に伴う決済処理は、情報提供サーバ10と決済処理サーバ14との間で行われる。モバイル・エレクトロニックコマース・サービスの詳細については、後で詳しく説明する。

#### 【0044】

モバイル・エレクトロニックコマース・サービスにおいて、本システムの各機器間で行われるデータ通信は、次に示す伝送路または通信回線を用いて行われる。まず、モバイルユーザ端末101は、伝送路108とインターネット100とデジタル通信回線110とを介して情報提供サーバ102とデジタル通信を行い、伝送路108とインターネット100とデジタル通信回線111とを介して電子バリュー発行サーバ103とデジタル通信を行い、伝送路108とインターネット100とデジタル通信回線111とを介してサービスサーバ106とデジタル通信を行い、伝送路109を介してサービス端末105と赤外線通信を行う。また、モバイルユーザ端末101と電子バリュー発行サーバ103との通信、モバイルユーザ端末101とサービス端末105との通信、モバイルユーザ端末1

01とサービスサーバ106との通信では、交換される情報を、全て、暗号化して通信する。暗号化には、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを組合わせて、情報を電子封書化して通信する。

【0045】

次に、本システムを構成する各構成要素について説明する。まず、サービス端末105について説明する。図6は、サービス端末105のブロック構成図である。図6において、サービス端末105は、コンピュータ600と無線通信モデム601と赤外線通信アダプタ602によって構成される。サービス端末105には、デジタル無線通信と赤外線通信の2系統の通信機能があり、デジタル無線通信機能によってインターネットアクセスを行い、赤外線通信機能によってモバイルユーザ端末との電子バリューの改札決済処理を行う。コンピュータ600には、マーチャントアプリケーションが搭載されており、このマーチャントアプリケーションに基づいて、コンピュータ600が無線通信モデム601と赤外線通信アダプタ602を制御して、電子バリューの改札決済処理を行う。同様に、サービスサーバ106にも、マーチャントアプリケーションが搭載されており、サービスサーバ106は、このマーチャントアプリケーションに基づいて、電子バリューの改札決済処理を行う。改札決済処理におけるサービス端末105とサービスサーバ106の詳細な動作とについては、後で詳しく説明する。

【0046】

次に、ユーザ端末107について説明する。図7は、ユーザ端末107のブロック構成図である。図7において、ユーザ端末107は、コンピュータ700とスマートカードリーダーライタ701と通信モデム702によって構成される。ユーザ端末107には、ブラウザアプリケーションプログラムと電子財布アプリケーションプログラムが搭載されており、インターネットへのアクセスは通信アダプタ702によって行う。ユーザ端末107は、スマートカードリーダーライタ701に、モバイルユーザ端末101のスマートカードを挿入することにより、サービス端末105との改札決済処理を除いて、モバイルユーザ端末101と同じ機能を持つ。

【0047】

次に、モバイルユーザ端末 101 について説明する。図 2 (a)、図 2 (b) は、それぞれ、モバイルユーザ端末 101 の前面側及び背面側の外観図である。図 2 (a) において、211 は、サービス端末 105 と赤外線通信を行なう赤外線通信ポート（赤外線通信モジュール）、210 は、デジタル無線通信の電波を受発信するアンテナ、209 は、レシーバスピーカ、200 は、120×160 画素表示のカラー液晶ディスプレイ（LCD）、203 は、通話スイッチ、202 は、通話の終了スイッチと電源スイッチを兼ねた終了／電源スイッチ、204 は、ナビゲーションスイッチ、205 と 206 はファンクションスイッチ、201 は、テンキースイッチ、207 は、マイクである。さらに、図 2 (b) において、212 は、スマートカードスロット（スマートカードリーダーライタ）である。

【0048】

モバイルユーザ端末 101 には、デジタル無線通信と赤外線通信の 2 系統の通信機能があり、デジタル無線通信機能によって音声通話とインターネットアクセス、及びサービスサーバとの電子バリューの改札決済処理を行い、赤外線通信機能によってサービス端末との電子バリューの改札決済処理を行う。さらに、モバイルユーザ端末 101 には、ブラウザ機能と電子財布機能があり、ブラウザ機能によってインターネットとモバイルユーザ端末のローカルデータのブラウジングを行い、電子財布機能によって電子バリューの管理、及び改札決済処理を行う。図 3 は、モバイルユーザ端末 101 のブロック構成図である。図 3 において、モバイルユーザ端末 101 は、FeRAM (Ferroelectric Random Access Memory) 301 に格納されたプログラムにしたがって、FeRAM 301 に格納されたデータの処理と送受信データの処理、並びにバス 306 を介して他の構成要素の制御を行なう CPU (Central Processing Unit) 300 と、LCD 100 と、赤外線通信モジュール 111 と、スマートカードリーダーライタ 112 と、テンキースイッチ 101、終了／電源スイッチ 102、通話スイッチ 103、ナビゲーションスイッチ 104、及びファンクションスイッチ 105、106 と、スイッチ操作を検出するキー制御部 302 と、スピーカ 303 とレシーバ 109 をドライブレマイク 107 から入力するアナログ音声信号をデジタル処理する音声処理部 304 と、アンテナ 110 を介して行う無線データ通信及び無線音声通信を制御

する無線通信部 305 と、スマートカード 307 とによって構成される。

【0049】

スマートカード 307 は、CPU と不揮発性メモリを内蔵し、不揮発性メモリには、ユーザの UPT (Universal Personal Telecommunication) 番号 (電話番号) と、モバイル・エレクトロニックコマース・サービスにおけるユーザ ID と、~~公開鍵暗号方式のユーザ秘密鍵と、それに対応するユーザ証明書、並びに、サービス提供者証明書 (サービス提供者のデジタル証明書) と、ユーザが購入した電子バリューと、電子バリューの購入及び改札決済処理の領収書が格納される。~~ FeRAM 301 には、OS (Operating System) と電話の他に、ブラウザと電子財布の 2 つのアプリケーションプログラムが格納されており、CPU 300 は、これらのアプリケーションを同時に実行する。

【0050】

図 4 は、CPU 300 が実行するアプリケーション (ブラウザと電子財布) と、モバイルユーザ端末 101 の他の構成要素と、他の機器との関係を示す模式図である。図 4 において、CPU 300 は、ブラウザ 401 と電子財布 400 の 2 つのプロセスを実行する。ブラウザ 401 は、キー制御部 302 から送られるユーザ操作情報 (スイッチ操作) に基づいて、無線通信部 305 を用いて、情報提供サーバ 103 とインターネット 100 を介して通信し、情報提供サーバ 103 から受信したデータを解釈して、LCD 200 に表示する。この時、情報提供サーバ 103 から受信するデータは、特定のマークアップ記述言語に基づいて記述されており、ブラウザ 401 は、このマークアップ記述言語を解釈して画像データを生成し、LCD 200 に表示する。また同様に、ブラウザ 401 は、FeRAM 301 に格納されたファイルや、電子財布 400 から受信したデータを解釈し、LCD 200 に表示する。この時、FeRAM 301 に格納されたファイル、及び電子財布 400 から受信したデータは、特定のマークアップ記述言語に基づいて記述されている。例えば、図 5 (a) は、電源をオンした時に LCD 200 に表示されるマイメニュー画面を示している。終了/電源スイッチ 202 によって電源をオンすると、ブラウザ 401 は、まず、FeRAM 301 に格納されたマイメニューファイルを読み出し、図 5 (a) に示す画面を表示する。マイメ

ニューファイルは、モバイルユーザ端末 1 0 1 の操作メニューであり、特定のマークアップ記述言語に基づいて記述されている。

【 0 0 5 1 】

ここで例えば、" 1 Internet"を選択すると、ブラウザ 4 0 1 は、インターネットにアクセスし、" 1 Internet"にリンクされた図 5 (b) に示すインターネットメニュー画面を表示する。ユーザは、このインターネットメニュー画面からインターネット上のサイト、例えば情報提供サーバ 1 0 2 にアクセスをする。図 5 (c) は、情報提供サーバ 1 0 2 にアクセスし、電子バリューをオーダーする場合の画面の一例を示している。また、" 2 E-Wallet"を選択すると、ブラウザ 4 0 1 は、電子財布 4 0 0 にアクセスし、電子財布 4 0 0 から受信したデータに基づいて、図 5 (d) に示すパスワードの入力を要求する画面を表示する。さらにこの画面でパスワードを入力すると、ブラウザ 4 0 1 は、入力されたパスワードを電子財布 4 0 0 に送信し、パスワードが正しい場合、電子財布 4 0 0 からブラウザ 4 0 1 に、電子財布 4 0 0 で管理されている電子バリューの一覧を示すデータが送信され、ブラウザ 4 0 1 は、図 5 (e) に示す画面を表示する。パスワードが間違っている場合には、エラー画面が表示される。さらに、" 7 Soccer 2 0 0 X Japa" を選択すると、電子財布 4 0 0 からブラウザ 4 0 1 に、選択された電子バリューの内容を示すデータが送信され、ブラウザ 4 0 1 は、図 5 (f) に示す画面を表示する。以上において、電子財布 4 0 0 からブラウザ 4 0 1 に送信されるデータは、特定のマークアップ記述言語に基づいて記述されている。

【 0 0 5 2 】

図 5 (a) ~ (f) に示すように、ブラウザ 4 0 1 が LCD 2 0 0 に表示する画面は、受信したデータを表示するコンテンツ表示領域 5 0 0 と、画面上部の状態表示領域 5 0 2 と、画面下部のメニュー表示領域 5 0 2 の 3 つの領域に分けられる。状態表示領域 5 0 2 には、現在、どこと通信しているか、及び通信がセキュアか否かが示される。例えば、図 5 (c) の場合には、表示されている画面がインターネットをアクセスしたもので、その通信がセキュアな通信で盗聴されないことを示している。また、図 5 (e) の場合には、表示されている画面が電子財布 4 0 0 をアクセスしたもので、ブラウザ 4 0 1 と電子財布 4 0 0 間の通信

がセキュアな通信で盗聴されないことを示している。メニュー表示領域 502 は、表示中の画面において、ファンクションスイッチ 205、206 に割り当てられたファンクションを示す領域である。例えば、図 5 (a) の場合には、ファンクションスイッチ 205 に "OK" つまり「選択」を意味するファンクションが割り当てられ、ファンクションスイッチ 206 に "back" つまり「戻る」を意味するファンクションが割り当てられる。

#### 【0053】

一方、電子財布 400 は、ブラウザ 401 からの要求に応じて、電子バリュー発行サーバ 103 からの電子バリューの受信と、スマートカード 307 に格納された電子バリューの管理、及びサービス端末 105 またはサービスサーバ 106 との改札決済処理を行う。例えば、図 5 (a) のマイメニュー画面で、ユーザが "2 E-Wallet" を選択した場合、"2 E-Wallet" には、"wallet:///index" という URI (Uniform Resource Identifier) がリンクされており、ブラウザ 401 は電子財布 400 に電子財布内のインテックス情報つまり電子財布 400 で管理されている電子バリューの一覧を要求する。それに対し、電子財布 400 は、特定のマークアップ記述言語で記述されたパスワード入力画面データをブラウザ 401 に返し、次にブラウザからユーザが入力したパスワードが送信されると、スマートカードリーダー 212 を介してスマートカード 307 にアクセスし、スマートカード 307 に登録されたパスワードと照合してパスワードが正しい場合に、つまりユーザが認証された場合に、特定のマークアップ記述言語で記述されたスマートカード 307 に格納されている電子バリューの一覧を示すデータをブラウザ 401 に返す。

#### 【0054】

さらに、図 5 (e) の電子バリューの一覧画面で、ユーザが "7 Soccer 200X Japa" を選択した場合、"7 Soccer 200X Japa" には、"wallet:///Evaluate/ev00000033" という URI がリンクされており、ブラウザ 401 は電子財布 400 に "ev 00000033" という識別子で管理されている電子バリューを要求する。それに対し、電子財布 400 は、スマートカードリーダー 212 を介してスマートカード 307 にアクセスし、スマートカード 307 の

不揮発性メモリに“ev 00000033”という識別子で格納管理されている電子バリューデータから、電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューの内容を示すデータを要求し、電子バリューオブジェクトが生成した電子バリューの内容を示すデータを、ブラウザ401に返す。この時、電子バリューオブジェクトが生成する電子バリューの内容を示すデータは、特定のマークアップ記述言語に基づいて記述されている。

## 【0055】

また例えば、電子バリューの購入の場合には、電子財布400は、ブラウザ401からの電子バリューの受信要求に基づいて、電子バリュー発行サーバ103からの電子バリューを受信する。このブラウザからの電子バリューの受信要求には、電子バリュー発行サーバ103のURI (<http://www.evalue.com>) と、受信する電子バリューを示すセッション番号が含まれ、この電子バリュー発行サーバ103のURIとセッション番号は、ブラウザ401の情報提供サーバ102への電子バリューの購入オーダーに対して情報提供サーバ102からブラウザ401に送信される電子バリューの受信を指示するデータの中に含まれている。ブラウザ401から電子バリューの受信を要求され電子財布400は、無線通信部305を介して電子バリュー発行サーバ102にアクセスし、スマートカード307に格納されているユーザ秘密鍵とユーザ証明書とサービス提供者証明書を用いて、電子バリュー発行サーバ102との間で暗号化通信セッションを確立して、電子バリュー発行サーバ102に電子バリューの発行を要求し、電子バリュー発行サーバ102から電子バリューを含むデータを受信する。この時、電子財布から電子バリュー発行サーバに送信される電子バリューの発行要求には、電子財布が受信する電子バリューを示すセッション番号が含まれる。電子バリューを含むデータを受信した電子財布400は、受信したデータから電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューデータの生成を要求し、電子バリューオブジェクトが生成した電子バリューデータをスマートカード307に格納して、電子バリューを電子財布に登録する。ここで電子バリューデータとは、電子バリューオブジェクトを特定のフォーマットのシリアルデータに変換したものであり、また、そのシリアルデータに、さらに暗

号化を施したものであっても良い。

【0056】

また、電子バリューの改札決済処理の場合には、電子財布400は、ブラウザ401からの電子バリューの改札決済処理要求に基づいて、サービス端末105またはサービスサーバ106との間で改札決済処理を行う。ブラウザ401からの改札決済処理要求に対し、~~ブラウザ401がサービスサーバ106と通信中~~の場合には、電子財布400は無線通信部5a-05を介してサービスサーバ106と改札決済処理を行い、ブラウザ401がサービスサーバ106と通信していない場合には、電子財布400は赤外線通信モジュール2a-11を介してサービス端末105と改札決済処理を行う。電子バリューの改札決済処理については後で詳しく説明する。次に、スマートカード307に格納される電子バリュー（電子バリューデータ）のデータ構造について説明する。図8は、電子バリューのデータ構造を示す模式図である。図8において、一つの電子バリューは、バリュー属性記述部800、サービス制御部803、セキュリティ情報部804、表示制御部805、表示リソース部806の5つの部分から構成される。

【0057】

バリュー属性記述部800は、電子バリューのタイプ、コード番号、ID番号、名称など、各種属性を規定する部分であり、バリュー属性記述部800は、さらに、改札決済処理により値が変化しない固定属性を示すプレゼンテーションカード801と、改札決済処理により値が変化する可変属性802に分けられる。サービス制御部803は、電子バリューが改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部804は、電子バリューが持つ暗号鍵等の機密情報を規定する部分、表示制御部805は、電子バリューの表示を規定する部分、表示リソース部806は、電子バリューの表示及びサウンド効果に用いるイメージデータや音声データ等を規定する部分である。また、電子バリューのデータ構造は、特定のマークアップ記述言語に基づいており、スマートカード307には、それをさらにエンコードしたものが格納される。

【0058】

図12は、特定のマークアップ記述言語で記述された電子バリューの一例を、



一部省略して示しており、この場合、この電子バリューは、電子財布400に“ev00000033”という識別子で管理されている。プレゼンテーションカード801は、サービス提供者(<http://www.evalue.com>)によりデジタル署名されており、可変属性802は、この電子バリューの秘密鍵(ev Private Key)によって、つまり、この電子バリュー自身によってデジタル署名されている。また、サービス制御部803とセキュリティ情報部804と表示制御部805と表示リソース部806は、サービス提供者(<http://www.evalue.com>)によりデジタル署名されている。これらのデジタル署名は、電子バリューオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。ただし、表示制御部805と表示リソース部806は、そのURIのみ規定されており、表示制御部の実体は、1201の部分で、表示リソース部の実体は、1202の部分で、それぞれ個別に規定される。または、サービス提供者(<http://www.evalue.com>)についても、1200の部分で規定される。

【 0 0 5 9 】

図１３は、図１２に示した電子バリューのプレゼンテーションカード８０１と可変属性８０２を省略無しに示したものである。図１３によれば、この電子バリューには、固定属性として、電子バリューのタイプ(evType)がチケット(ticket)で、コード番号(evCode)が、

" 0 0 0 0 3 0 0 0 0 0 0 0 0 2 0 1 "

また、ID番号(evID)が、

" 1 0 1 "

チケットのタイトル(TITLE)が、

" Soccer 2 0 0 X Japan vs Brazil"

席番号(SEAT\_NUM)が、

"SS-A-2 8"

等の属性があり、また可変属性として、

有効性フラグ (VALIDITY) が " 1 " (つまり有効) で、

使用済フラグ(USED)が” 0 ” (つまり未使用) で、

回数券枚数(NUMBER)が” 1 ” (つまり 1 回使い切りのチケット)

といった属性を持っている。

【0060】

図14は、図12に示した電子バリュウのサービス制御部803とセキュリティ情報部804を省略無しに示したものである。図14によれば、この電子バリュウには、チケットモジュール(ticket)と属性検証モジュール(verify\_prop)とメッセージ設定モジュール(set\_message)の3つのサービス制御モジュールが規定されている。ここで、サービス制御モジュールとは、改札決済処理で行う処理を、小さな処理モジュールに部品化したものである。改札決済処理では、サービス制御部803に規定されたサービス制御モジュールがそれぞれ実行される。つまり、サービス制御部803に規定するサービス制御モジュールの組合わせを変えることによって、各種の改札決済処理を規定することが出来る。例えば、この電子バリュウの場合、チケットモジュールは、チケットの基本機能をモジュール化したものであり、改札決済処理によって、チケットの回数券枚数(\$NUMBER)を"1"デクリメントし、有効期間の開始日時(\$START\_VALID)と終了日時(\$END\_VALID)をそれぞれ設定し、使用済フラグ(\$USED)を"1"(つまり使用済)に、有効性フラグ(\$VALIDITY)を有効期間に応じて設定し、電子バリュウを使用した回数、つまり改札決済処理の回数を示す使用シリアル番号(\$USE\_SERIAL)を"1"インクリメントする。属性検証モジュールは、指定された電子バリュウの属性を検証するモジュールであり、この場合、改札決済処理によって席番号(\$SEAT\_NUM)が検証される。

【0061】

メッセージ設定モジュールは、メッセージ(文字列)を設定するモジュールであり、改札決済処理によって、可変属性の1つであるメッセージ2(\$MESSAGE\_2)に、サービス端末105(または、サービスサーバ106)に設定されたメッセージが設定される。以上の処理が、1回の改札決済処理の中で、同時に行われる。また、セキュリティ情報部804には、この電子バリュウ固有の鍵である公開鍵暗号方式の電子バリュウ秘密鍵(evPrivateKey)と、それに対応する電子バリュウ証明書(evCertificate)、並びに、電子バリュウのコード番号毎に固有の鍵である共通鍵方式の電子バリュウ認証鍵(evAuthKey)と電子バリュウハンド

ラ認証鍵(evhandlerAuthKey)等が規定されている。ここで、電子バリューハンドラとは、この電子バリューと改札決済処理を行うサービス端末105またはサービスサーバ106に、予め設定されている改札決済処理のための情報である。サービス端末105またはサービスサーバ106では、改札決済処理時に、この情報から電子バリューハンドラオブジェクトが生成され、実質的に、電子バリューオブジェクトと電子バリューハンドラオブジェクトとの間で改札決済処理が行われる。電子バリューハンドラについては、後で詳しく説明する。

#### 【0062】

図15は、図12に示した電子バリューの表示制御部805を省略無しに示したものである。図15によれば、この電子バリューには、“Main”と“Detail”の2つの画面情報が規定されている。表示制御部805には、マークアップ記述言語による表示画面のテンプレートが規定されている。この電子バリューの電子バリューオブジェクトは、`<evP>`と`</evP>`に挟まれた部分をプレゼンテーションカード801で規定されている属性の値に、`<evV>`と`</evV>`に挟まれた部分を可変属性802で規定されている属性の値に、それぞれ置きかえることによって、電子バリューの内容を示すデータを生成する。例えば、図5(e)の電子バリューの一覧画面で、ユーザが“7 Soccer 200X Japa”を選択した場合には、電子バリューオブジェクトは、図17に示す“Main”の画面情報を生成し、ブラウザ401によって、LCD200には、図5(f)に示す画面が表示される。

#### 【0063】

図16は、図12に示した電子バリューの表示リソース部806を省略無しに示したものである。図16によれば、この電子バリューには、“MAIN\_IMG”と“MAP”というラベルが付けられた2つのイメージデータと、“Greet”というラベルが付けられた1つの音声データが規定されている。例えば、図17に示した“Main”の画面情報の場合、“`<IMG SRC=wallet:///evResource label=MAIN_IMG>`”の部分は、電子財布400に存在する電子バリューオブジェクトの表示リソース部の中のラベルが“MAIN\_IMG”のイメージの表示を規定している記述であり、図16に示したリソースデータの内、“MAIN\_IMG”というラベルが付いたイメージデータが、ブラウザ401に送られ、図5(f)に示すような画面が表示され

る。このように、一つの電子バリューが持つ各種の属性、改札決済処理で行う処理の内容、及び電子バリューの表示は、このようなマークアップ記述言語に基づいて規定される。

#### 【0064】

なお、電子バリューの表示制御部の実体 1201 と表示リソース部の実体 1202 は、スマートカード 307 に格納せずに、FeRAM 301 に格納しするようにしても良い。この場合、スマートカード 307 に、より多くの電子バリューを格納することが出来るというメリットがある。ただしこの場合、ユーザ端末 107 のスマートカードリーダーライタ 701 にスマートカード 307 を挿入して、コンピュータ 700 の画面に電子バリューの内容を表示する際、表示制御部の実体 1201 と表示リソース部の実体 1202 が必要になるが、表示制御部 805 と表示リソース部 806 に規定されているそれらの実体の URI を基に、インターネット 100 を介して表示制御部の実体 1201 と表示リソース部の実体 1202 をダウンロードすることにより、電子バリューの内容を表示することが出来る。

#### 【0065】

次に、電子バリューハンドラについて説明する。電子バリューハンドラは、電子バリューのコード番号に対応して存在し、サービス提供者によって、予め、その電子バリューを取り扱うマーチャントのサービス端末 105 及びサービスサーバ 106 に対して、インターネット 100 を介して配布されている。図 9 は、電子バリューハンドラのデータ構造を示す模式図である。図 9 において、一つの電子バリューハンドラは、バリュー属性記述部 900、サービス制御部 903、セキュリティ情報部 904 とマーチャントオプション 905 の 4 つの部分から構成される。バリュー属性記述部 900 は、取り扱う電子バリューのタイプ、コード番号、ID 番号、名称など、各種属性を規定する部分で、サービス制御部 903 は、電子バリューとの改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部 904 は、電子バリューハンドラが持つ暗号鍵等の機密情報を規定する部分、マーチャントオプション 905 は、マーチャント独自の追加設定を規定する部分である。電子バリューハンドラもまた、そのデータ構造は、特

定のマークアップ記述言語に基づいており、サービス端末105またはサービスサーバ106には、それをさらにエンコードしたものが格納される。

#### 【0066】

図18は、図12に示した電子バリューに対応する電子バリューハンドラのマークアップ記述言語による記述を一部省略して示しており、この場合、この電子バリューハンドラは、電子マーチャントに“ev 00000001”という識別子で管理されている。電子バリューハンドラを構成するデータの内、バリュー属性記述部900とサービス制御部903とセキュリティ情報部904がサービス提供者から配布されたものであり、マーチャントオプション905は、マーチャントがマーチャントアプリケーションによって追加設定したものである。したがって、バリュー属性記述部900とサービス制御部903とセキュリティ情報部904の部分にのみ、サービス提供者 (<http://www.evalue.com>) によるデジタル署名が施されている。このデジタル署名は、電子バリューハンドラオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。

#### 【0067】

図18のバリュー属性記述部900によれば、取り扱う電子バリューは、電子バリューのタイプ(evType)がチケット(ticket)で、コード番号(evCode)が“0000300000000201”、チケットのタイトル(TITLE)が“Soccer 200X Japan vs Brazil”といった属性を持っている。ただし、席番号(SEAT\_NUM)とメッセージ2(MESSAGE\_2)に関しては規定されておらず、それぞれには、電子バリューハンドラの所有者(マーチャント)による設定を許可するpermission=“public”という要素が付加されている。これにより、マーチャントによるマーチャントオプション905の追加が可能になり、例えば、図18のマーチャントオプション905では、席番号(\$SEAT\_NUM)に“SS-\*-\*”が、メッセージ2(\$MESSAGE\_2)に“Special News available: <http://www.yis.co.jp/news/20020630>”がそれぞれ設定されている。

#### 【0068】

図18のサービス制御部903には、電子バリューのチケットモジュール(tic

ket)と属性検証モジュール(verify\_prop)とメッセージ設定モジュール(set\_message)に対応するサービスモジュールが規定されている。マークアップ記述言語による記述は電子バリューと同じであるが、それぞれ、マーチャント側の処理を行うサービスモジュールが実行される。例えば、属性検証モジュールの場合には、マーチャントオプション905の設定にしたがって、席番号(\$SEAT\_NUM) が、"SS-\*\*-\*\*"と照合される。この時、'-\*\*'は任意の文字列を意味し、SS席のチケットのみ、改札決済処理が可能となる。また、メッセージ設定モジュールの場合には、マーチャントオプション905の設定にしたがって、改札決済処理により、電子バリュー側のメッセージ2(\$MESSAGE\_2)に"Special News available: <http://www.yis.co.jp/news/20020630>"というメッセージが設定される。

#### 【0069】

図18のセキュリティ情報部904には、図12に示した電子バリューのセキュリティ情報部804に規定されているものと同じ電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)が規定されている。電子バリューと電子バリューハンドラは、改札決済処理の際、この電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)を用いて相互認証を行う。

#### 【0070】

次に、モバイルユーザ端末101とサービス端末105間の改札決済処理について説明する。改札決済処理は、ユーザが使用する電子バリューをLCD200に表示し、赤外線通信ポート(赤外線通信モジュール)をサービス端末105の赤外線通アダプタ602に向けて、改札決済処理の実行に割り付けられたファンクションスイッチを押すことによって開始する。例えば、図17に示した"Main"の画面の場合、改札決済処理の実行に割り付けられたファンクションスイッチを押すことによって、<Go HREF="wallet:///evTransact"/>が実行され、電子財布400上の電子バリューオブジェクトに改札決済処理が要求される。

#### 【0071】

図10は、改札決済処理においてモバイルユーザ端末101とサービス端末1

05間で交換されるメッセージを示している。まず、電子バリューオブジェクトから電子バリューの改札決済処理を申し出るメッセージ、プレゼンテーション (Presentation) 1003が送信される。それに対し、サービス端末105のマーチャントアプリケーションは、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリューハンドラオブジェクトから電子バリューに属性の値の変更を要求するメッセージ、インストラクション (Instruction) 1004が送信される。電子バリューオブジェクトは、インストラクション1004に基づいて属性の値を変更し、その変更を証明するメッセージ、トランザクション (Transaction) 1005を電子バリューハンドラオブジェクトに送信する。電子バリューハンドラオブジェクトは、トランザクション1005の内容を検証し、正しい場合に、トランザクション1005の領収書に相当するレシート (Receipt) 1006を送信する。さらに、電子バリューオブジェクトは、レシート1006の内容を検証し、正しい場合に、レシート1006の受け取り確認 (アクノレッジ) に相当するメッセージ、アクノレッジ (Acknowledge) 1007を電子バリューハンドラオブジェクトに送信し、属性の値が変更された電子バリューデータとレシートをスマートカード a5-07に保存して改札決済処理を終了する。改札決済処理の途中で、エラーが発生した場合には、相手側にエラーメッセージを送信して改札決済処理を中止する。

## 【0072】

プレゼンテーション1003は、図11(a)に示すように、メッセージのヘッダ1110と、この改札決済処理を電子財布 a6-00からみてユニークに示す要求番号1111と、電子バリューのプレゼンテーションカード1012(801)と、サービス制御モジュールによるサービス制御メッセージ1113に、電子バリュー秘密鍵による電子バリュー署名 a14-14をし、さらに電子バリュー証明書1115を付加して、これを電子バリューハンドラ認証鍵で暗号化して、さらにメッセージのヘッダ1117と電子バリューのコード番号1118を付加したものである。サービス端末105のマーチャントアプリケーションは、プレゼンテーション1003のコード番号1118に基づいて、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリュー

ハンドラオブジェクトは、まず、電子バリューハンドラ認証鍵によって暗号化されている部分 1116 を復号化し、電子バリュー証明書 1115 さらには電子バリュー署名 a14-14 を検証して、サービス制御メッセージ 1113 を検証する。プレゼンテーション 1003 の検証結果が正しい場合に、電子バリューハンドラオブジェクトはインストラクション 1004 を生成、送信する。

---

【0073】

インストラクション 1004 は、図 11 (b) に示すように、メッセージのヘッダ 1120 と、プレゼンテーション 1003 に含まれていた要求番号 1121 (1111) と、この改札決済処理をマーチャントアプリケーションからみてユニークに示す決済番号 1112 と、サービス制御モジュールによるサービス制御メッセージ 1123 に、マーチャント秘密鍵によるマーチャント署名 a14-24 をし、さらにマーチャント証明書 1825 と、新たに生成したセッション鍵 A 1126 を付加して、これを電子バリュー認証鍵で暗号化して、さらにメッセージのヘッダ 1128 を付加したものである。電子バリューオブジェクトは、まず、電子バリュー認証鍵によって暗号化されている部分 1127 を復号化し、電子マーチャント証明書 1125 さらにはマーチャント署名 a14-24 を検証して、要求番号 1111 を照合し、サービス制御メッセージ 1113 を検証する。インストラクション 1004 の検証結果が正しい場合、はじめて、電子バリューハンドラオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューハンドラオブジェクトであると判定し、電子バリューオブジェクトは、インストラクション 1004 に基づいて属性の値を変更し、トランザクション 1005 を生成、送信する。トランザクション 1005 は、図 11 (c) に示すように、メッセージのヘッダ 1130 と、要求番号 1131 と、インストラクション 1004 に含まれていた決済番号 1132 (1122) と、トランザクション 1005 の宛先に相当するマーチャント ID 1133 と、サービス制御モジュールによるサービス制御メッセージ 1134 に、電子バリュー秘密鍵による電子バリュー署名 a14-35 をし、新たに生成したセッション鍵 B 1136 を付加して、これをインストラクション 1004 に含まれていたセッション鍵 A 1126 で暗号化して、さらにメッセージのヘッダ 1138 を付加した



ものである。

【0074】

電子バリューハンドラオブジェクトは、まず、セッション鍵A1126によって暗号化されている部分1137を復号化し、電子バリュー署名a14-35を検証して、要求番号1111及び決済番号1132を照合し、サービス制御メッセージ1113を検証する。トランザクション1005の検証結果が正しい場合、はじめて、電子バリューオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであると判定し、電子バリューハンドラオブジェクトは、トランザクション1005の領収書に相当するレシート1006を生成、送信する。

【0075】

レシート1006は、図11(d)に示すように、メッセージのヘッダ1140と、要求番号1141(1131)と、決済番号1142(1132)と、レシート1006の宛先に相当する電子バリューID1143と、サービス制御モジュールによるサービス制御メッセージ1144と、領収書情報1145とに、マーチャント秘密鍵によるマーチャント署名a14-46をし、さらに、トランザクション1005に含まれていたセッション鍵B1136で暗号化して、さらにメッセージのヘッダ1148を付加したものである。電子バリューオブジェクトは、まず、セッション鍵B1136によって暗号化されている部分1147を復号化し、マーチャント署名a14-46を検証して、要求番号1111及び決済番号1132を照合し、サービス制御メッセージ1113を検証する。レシート1006の検証結果が正しい場合、電子バリューオブジェクトは、正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであると判定し、電子バリューハンドラオブジェクトは、レシート1006の受け取り確認に相当するアクノレッジ1007を生成、送信する。

【0076】

アクノレッジ1007は、図11(e)に示すように、メッセージのヘッダ1150に、レシート1006に対する電子バリュー秘密鍵による電子バリュー署名a14-51を付加したものである。電子バリューハンドラオブジェクトは、

電子バリュー署名 a 14-51 を検証して、正しい場合に、復号化されたトランザクションとレシートを保存して改札決済処理を終了する。一方、アクノレッジ 1007 を送信した電子バリューオブジェクトは、属性の値を変更した電子バリューデータと、復号化されたレシートをスマートカード a 5-07 に保存して改札決済処理を終了する。この際、電子バリューの可変属性 802 には、電子バリュー秘密鍵によって新たにデジタル署名が施される。

## 【0077】

また、この改札決済処理において、プレゼンテーション 1003 とインストラクション 1004 とトランザクション 1005 とレシート 1006 の各メッセージに設定されるサービス制御メッセージによって、各電子バリューに固有の改札決済処理が行われる。サービス制御メッセージは、サービス制御モジュールによって設定され、相手側のサービス制御モジュールによって検証される。プレゼンテーション 1003 とインストラクション 1004 とトランザクション 1005 とレシート 1006 には、それぞれ、図 19 (a)、(b)、(c)、(d) に示すデータをエンコードしたものが、サービス制御メッセージとして設定される。例えば、図 19 (a) の場合、電子バリューハンドラオブジェクト側の ID が "1" のサービス制御モジュール (チケットモジュール) に対し `number= 1 start="1999.07.23T00:00+0900" end="2002.06.30T23:59+0900" used__flag= 0 validity__flag= 1 serial=0`、ID が "2" のサービス制御モジュール (属性検証モジュール) に対し `prop=SS-A-28`、ID が "3" のサービス制御モジュール (メッセージ設定モジュール) に対し `msg=` というように、現状の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。例えばこの時、電子バリューハンドラが図 18 に示したもので、`prop=S-A-28` であった場合には、照合エラーとなる。

## 【0078】

図 19 (b) の場合、電子バリューオブジェクト側の ID が "1" のサービス制御モジュール (チケットモジュール) に対し `number= 0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+`

0900" used \_\_flag= 1 validity\_\_flag= 1 serial=1、IDが" 3"のサービス制御モジュール（メッセージ設定モジュール）に対しmsg="Special News available: http://www.yis.co.jp/news/20020630" というように、属性の変更命令が提示され、電子バリューオブジェクトのそれぞれのサービス制御モジュールにおいて属性が変更される。

【0079】

図19（c）の場合、電子バリューハンドラオブジェクト側のIDが" 1"のサービス制御モジュール（チケットモジュール）に対しnumber= 0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900" used\_\_flag= 1 validity\_\_flag= 1 serial=1、IDが" 2"のサービス制御モジュール（属性検証モジュール）に対しprop=SS-A-28、IDが" 3"のサービス制御モジュール（メッセージ設定モジュール）に対しmsg="Special News available: http://www.yis.co.jp/news/20020630" というように、変更後の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。

【0080】

図19（d）の場合、電子バリューオブジェクト側のIDが" 1"のサービス制御モジュール（チケットモジュール）に対しserial= 1 というように、トランザクション1005の使用シリアル番号が提示され、電子バリューオブジェクトのチケットモジュールにおいて使用シリアル番号の照合が行われる。

【0081】

以上のようにして行われる改札決済処理の結果、例えば、図12に示した電子バリューの場合、可変属性は図20に示すようになる。特にこの場合、改札決済処理の結果、MESSAGE\_2には、"Special News available:http://www.yis.co.jp/news/20020630" というマーチャントが設定したメッセージが設定され、このメッセージは電子バリューの"Detail"画面表示においてLCD200に表示される。また、モバイルユーザ端末101とサービスサーバ106間の改札決済処理、及びユーザ端末107とサービスサーバ106間の改札決済処理は、赤外線通信がデジタル無線通信になる以外は同様の手順で行われる。

## 【0082】

以上のように、モバイルユーザ端末101とサービス端末105、及び電子バリューと電子バリューハンドラを構成することにより、各種の改札決済処理、つまり各種の電子バリューを規定することができ、また、安全性を確保しつつ、マーチャントの運用におけるある程度の自由な設定を可能に出来る。

## 【0083】

なお、以上に述べた構成では、モバイルユーザ端末101とサービス端末105との通信に赤外線通信を用いたが、その他の無線通信方式を用いてもよく、その場合、モバイルユーザ端末101は赤外線通信モジュール111の代わりにその無線通信方式の無線通信手段を、サービス端末105は、赤外線通信アダプタ602の代わりにその無線通信方式の無線通信手段をそれぞれ備える。また、以上の説明では、モバイル・エレクトロニックコマース・システムを構成するモバイルユーザ端末101は、モバイル・エレクトロニックコマース・サービスにおける機能を実現するための、最適なハードウェア構成を備えているが、機能としては、デジタル無線通信機能と、赤外線通信機能、及び、スマートカードリーダーライタと、ディスプレイと、キーボード（または、ペン入力デバイス）と、マイクと、スピーカとを備えたコンピュータによって構成することもできる。この場合、FeRAM301に格納されているプログラムを、パソコンのOS (Operating System) 上で動作するソフトウェア・プログラムに変換し、そのソフトウェア・プログラムを、コンピュータから実行可能な場所（例：ハードディスク）に格納しておく。

## 【0084】

## 【発明の効果】

以上のように、第1の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報とを備えた電子情報を、保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【0085】

第2の発明は、第1の発明の電子財布に、電子情報から電子情報オブジェクト

を生成し電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0086】

第3の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【0087】

第4の発明は、第3の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0088】

第5の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

## 【0089】

第6の発明は、第5の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0090】

第7の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【0091】

第8の発明は、第7の発明の電子財布に、電子情報から電子情報オブジェクト

を生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0092】

第9の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の可変の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

## 【0093】

第10の発明は、第9の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0094】

第11の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報に署名がされているので、発行者が規定した表示が保証される。

## 【0095】

第12の発明は、第11の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0096】

第13の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を電子財布が備えたものである。表示制御情報の識別情報に署名がされているので、発行者

が規定した表示が保証される。

【0097】

第14の発明は、第13の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

---

【0098】

第15の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示リソースの識別情報に署名がされているので、発行者が規定したイメージが保証される。

【0099】

第16の発明は、第15の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【0100】

第17の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報の識別情報および表示リソースの識別情報に署名がされているので、発行者が規定した表示が保証される。

【0101】

第18の発明は、第17の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0102】

第19の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証することができ、安全性が向上する。

---

## 【0103】

第20の発明は、第19の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0104】

第21の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0105】

第22の発明は、第21の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0106】

第23の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。



## 【0107】

第24の発明は、第23の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0108】

第25の発明は、固有の秘密鍵とその証明書組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

## 【0109】

第26の発明は、第25の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

## 【0110】

第27の発明は、サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せにしたものである。サービス制御モジュール情報の組合せを変更することにより、各種の電子情報を規定することが出来る。

第28の発明は、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御情報に基づく決済データを重畳するようにしたものがある。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

## 【0111】

第29の発明は、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御モジュール情報の組合せに基づく決済データを重畳するようにしたものである。決済処理時に交換するメッセージ数を変えること

無く、効率的な決済が可能となる。

【0112】

第30の発明は、電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

【0113】

第31の発明は、電子情報の表示手段を備えるようにしたものであり、電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【0114】

第32の発明は、電子情報から表示情報を生成する手段を備えるものであり、内容が変化した電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【0115】

第33の発明は、第1の発明から第32の発明に記載の電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録したものである。これにより、プログラムを、持ち運び可能な形態で、流通させることができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態におけるモバイル・エレクトロニックコマース・システムのブロック構成図

【図2】

(a) 本発明の実施の形態におけるモバイルユーザ端末の前面の概観図

(b) 本発明の実施の形態におけるモバイルユーザ端末の背面の概観図

【図3】

本発明の実施の形態におけるモバイルユーザ端末のブロック構成図

【図4】

本発明の実施の形態におけるモバイルユーザ端末のアプリケーションと他の構成要素と、他の機器との関係を示す模式図

【図 5】

(a) 本発明の実施の形態におけるモバイルユーザ端末の電源オン時の画面の概観図

~~(b) 本発明の実施の形態におけるモバイルユーザ端末のインターネットメニュー画面の概観図~~

(c) 本発明の実施の形態におけるモバイルユーザ端末の電子バリューのオーダー画面の概観図

(d) 本発明の実施の形態におけるモバイルユーザ端末のパスワード入力画面の概観図

(e) 本発明の実施の形態におけるモバイルユーザ端末の電子バリューの一覧画面の概観図

(f) 本発明の実施の形態におけるモバイルユーザ端末の電子バリュー表示画面の概観図

【図 6】

本発明の実施の形態におけるサービス端末のブロック構成図

【図 7】

本発明の実施の形態におけるユーザ端末のブロック構成図

【図 8】

本発明の実施の形態における電子バリューのデータ構造の模式図

【図 9】

本発明の実施の形態における電子バリューハンドラーのデータ構造の模式図

【図 10】

本発明の実施の形態における改札決済処理において交換されるメッセージの模式図

【図 11】

(a) 本発明の実施の形態における改札決済処理のメッセージ、プレゼンテーションのデータ構造の模式図

(b) 本発明の実施の形態における改札決済処理のメッセージ、インストラクションのデータ構造の模式図

(c) 本発明の実施の形態における改札決済処理のメッセージ、トランザクションのデータ構造の模式図

(d) 本発明の実施の形態における改札決済処理のメッセージ、レシートのデータ構造の模式図

---

(e) 本発明の実施の形態における改札決済処理のメッセージ、アクノレッジのデータ構造の模式図

【図 12】

本発明の実施の形態における電子バリューのマークアップ記述言語による記述の模式図

【図 13】

本発明の実施の形態における電子バリューのプレゼンテーションカードと可変属性のマークアップ記述言語による記述の模式図

【図 14】

本発明の実施の形態における電子バリューのサービス制御部とセキュリティ情報部のマークアップ記述言語による記述の模式図

【図 15】

本発明の実施の形態における電子バリューの表示制御部のマークアップ記述言語による記述の模式図

【図 16】

本発明の実施の形態における電子バリューの表示リソース部のマークアップ記述言語による記述の模式図

【図 17】

本発明の実施の形態における電子バリューオブジェクトが生成する"Main"の画面情報の模式図

【図 18】

本発明の実施の形態における電子バリューハンドラのマークアップ記述言語による記述の模式図

【図 1 9】

(a) 本発明の実施の形態における改札決済処理のメッセージ、プレゼンテーション中のサービス制御メッセージのデータ構造の模式図

(b) 本発明の実施の形態における改札決済処理のメッセージ、インストラクション中のサービス制御メッセージのデータ構造の模式図

(c) 本発明の実施の形態における改札決済処理のメッセージ、トランザクション中のサービス制御メッセージのデータ構造の模式図

(d) 本発明の実施の形態における改札決済処理のメッセージ、レシート中のサービス制御メッセージのデータ構造の模式図

【図 2 0】

本発明の実施の形態における改札決済処理後の電子バリューの可変属性のマークアップ記述言語による記述の模式図

【図 2 1】

(a) 従来の技術における電子化された価値情報が発行された状態を示す模式図

(b) 従来の技術における電子化された価値情報が使用された状態を示す模式図

【符号の説明】

- 1 0 0 インターネット
- 1 0 1 モバイルユーザ端末
- 1 0 2 情報提供サーバ端末
- 1 0 3 電子バリュー発行サーバ
- 1 0 4 決済処理サーバ
- 1 0 5 サービス端末
- 1 0 6 サービスサーバ
- 1 0 7 ユーザ端末
- 2 0 0 LCD
- 2 0 1 テンキースイッチ
- 2 0 2 終了／電源スイッチ

203 通話スイッチ

204 ナビゲーションスイッチ

205、206 ファンクションスイッチ

205 レシーバスピーカ

206 アンテナ

~~207 マイク~~

---

209 レシーバスピーカ

210 アンテナ

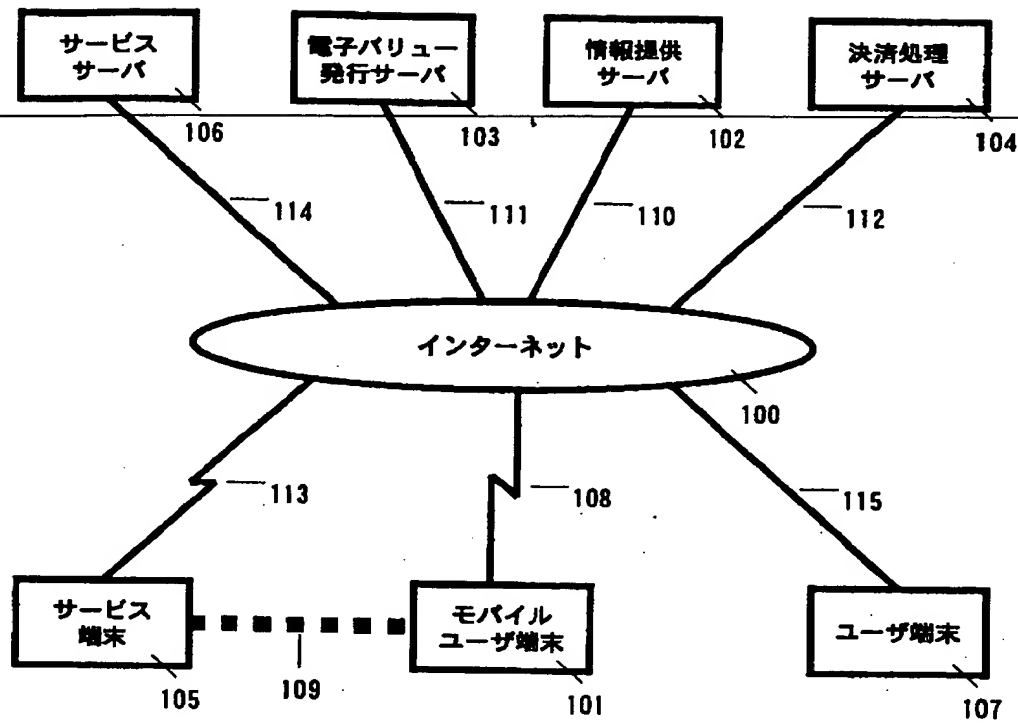
211 赤外線通信ポート（赤外線通信モジュール）

212 スマートカードスロット（スマートカードリーダーライター）

【書類名】

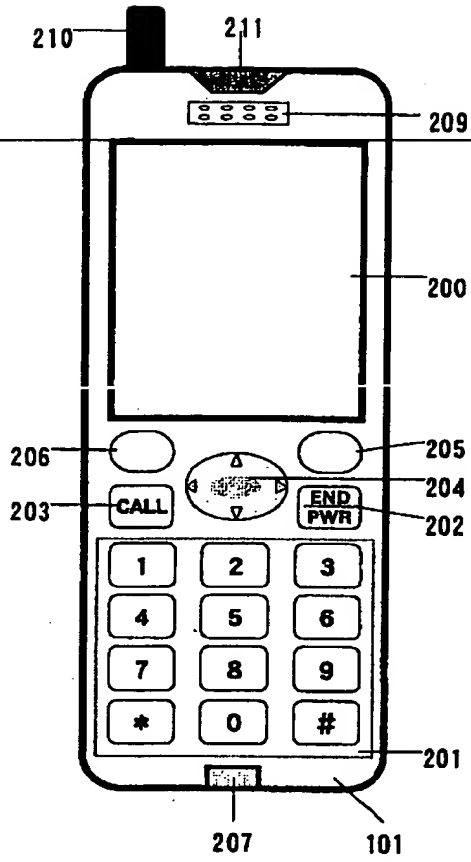
図面

【図 1】

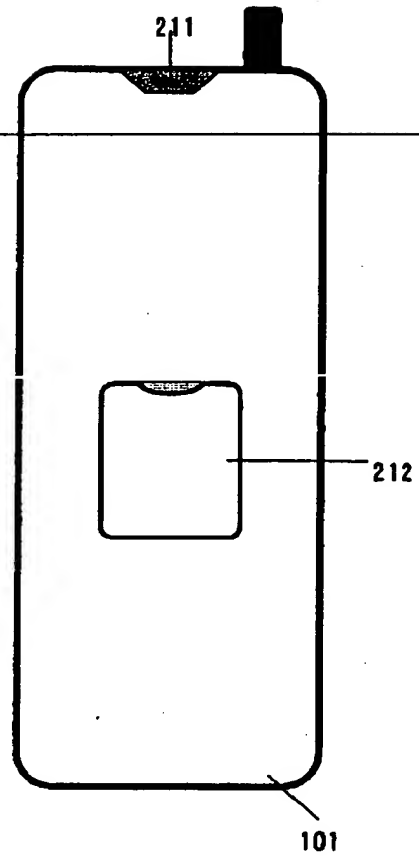


【図 2】

(a)

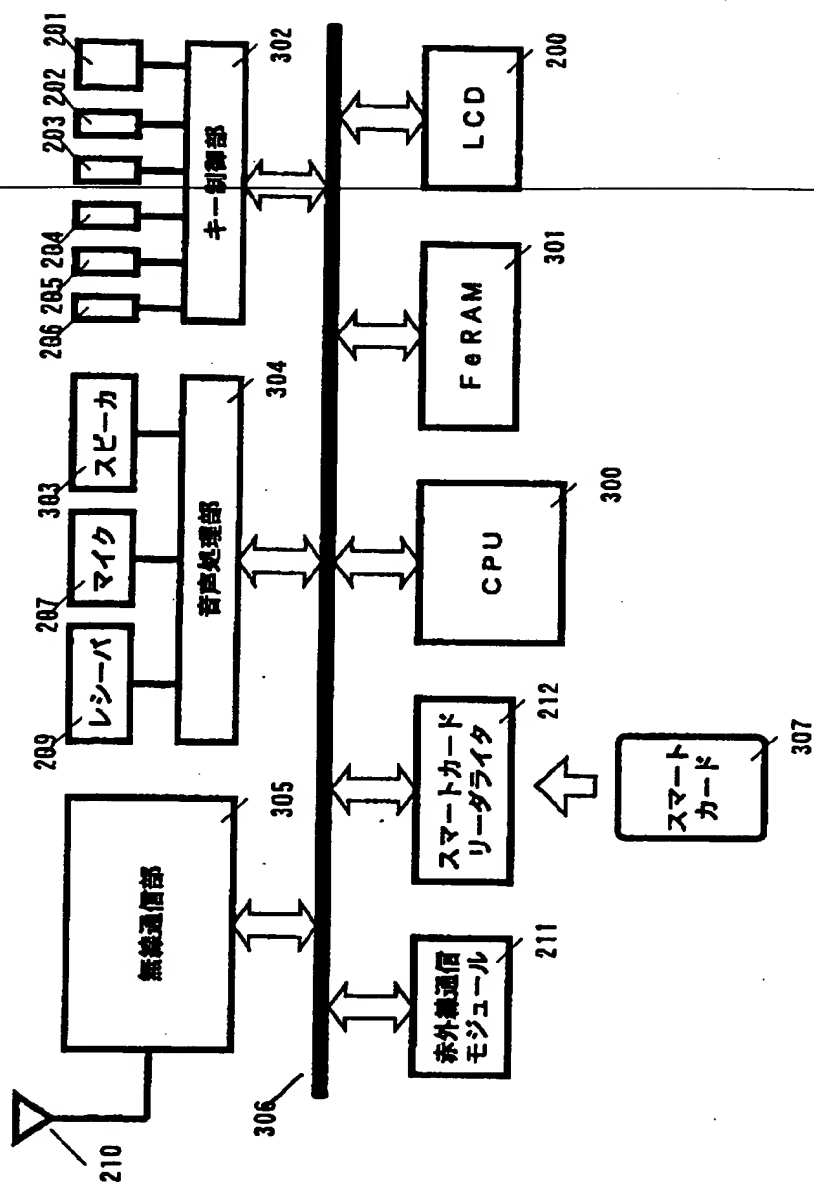


(b)

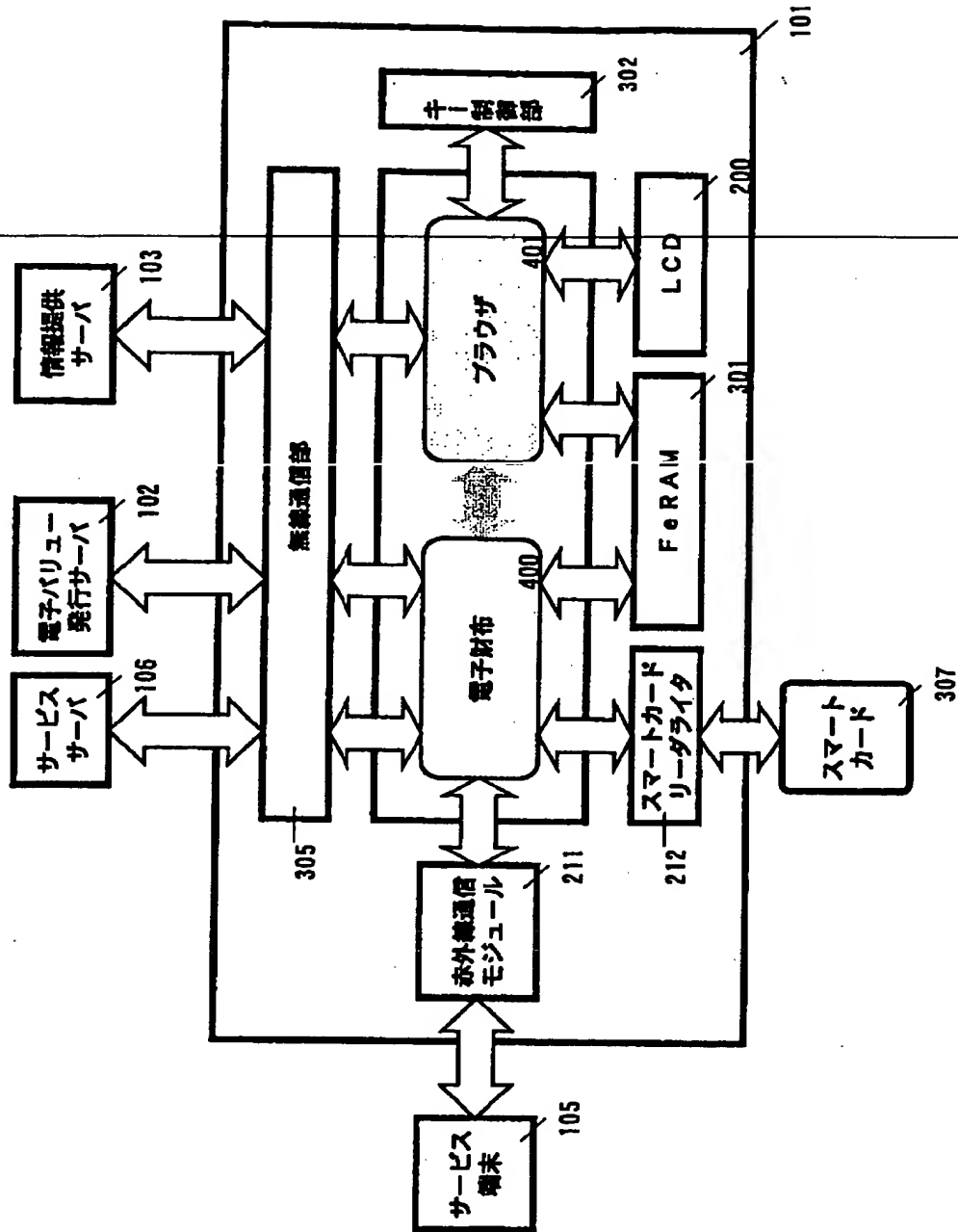




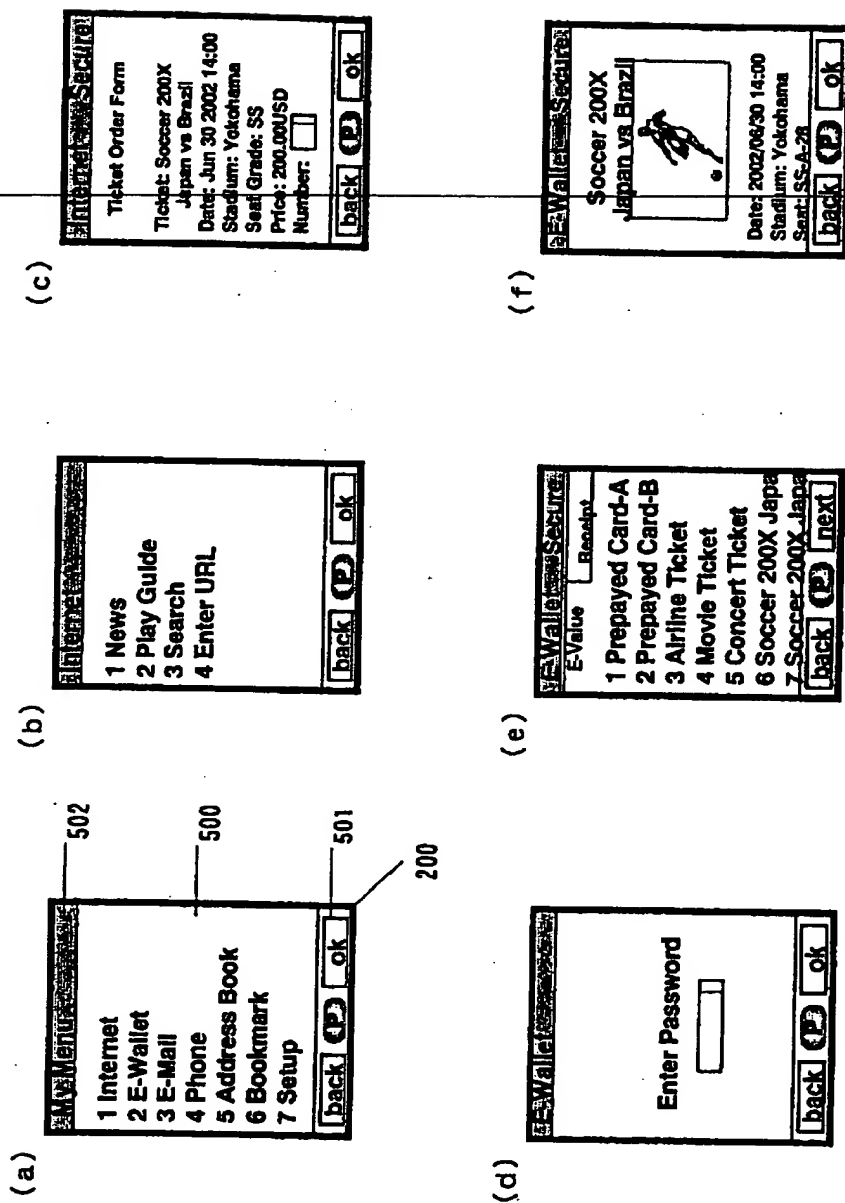
【図 3】



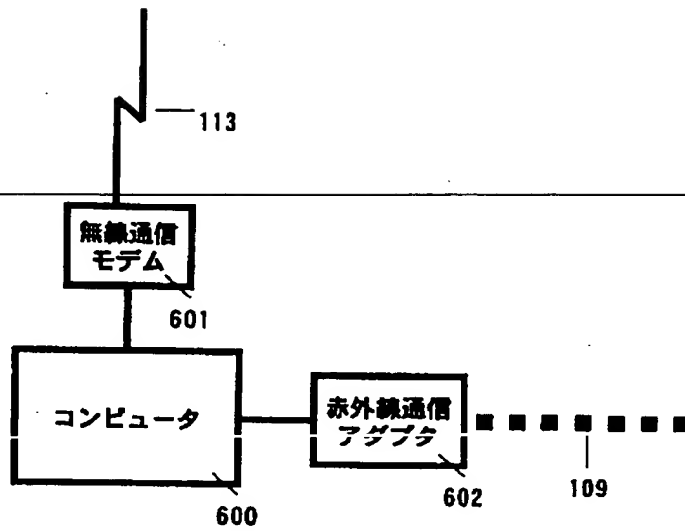
【図 4】



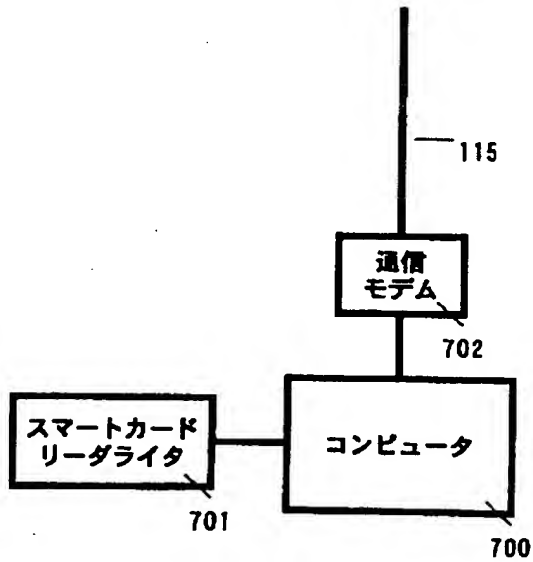
【図 5】



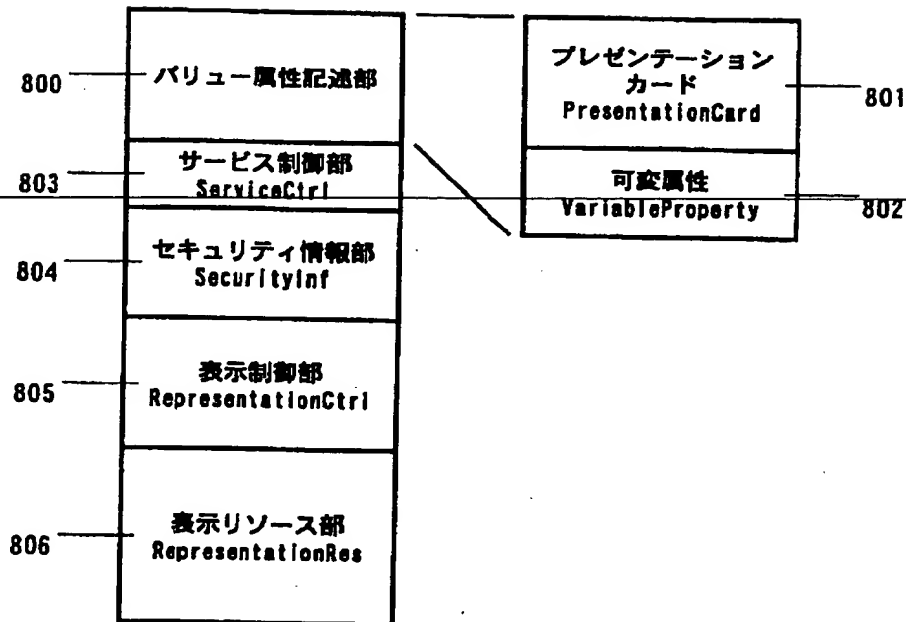
【図 6】



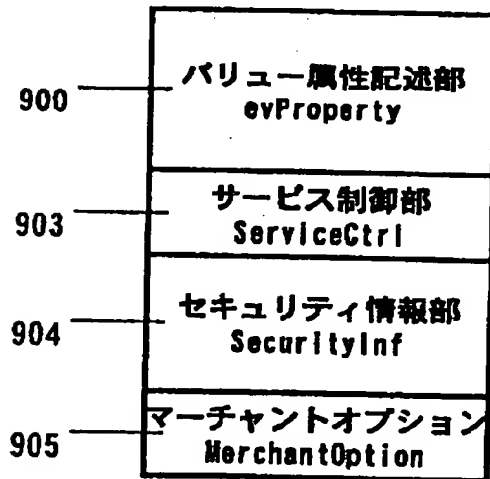
【図 7】



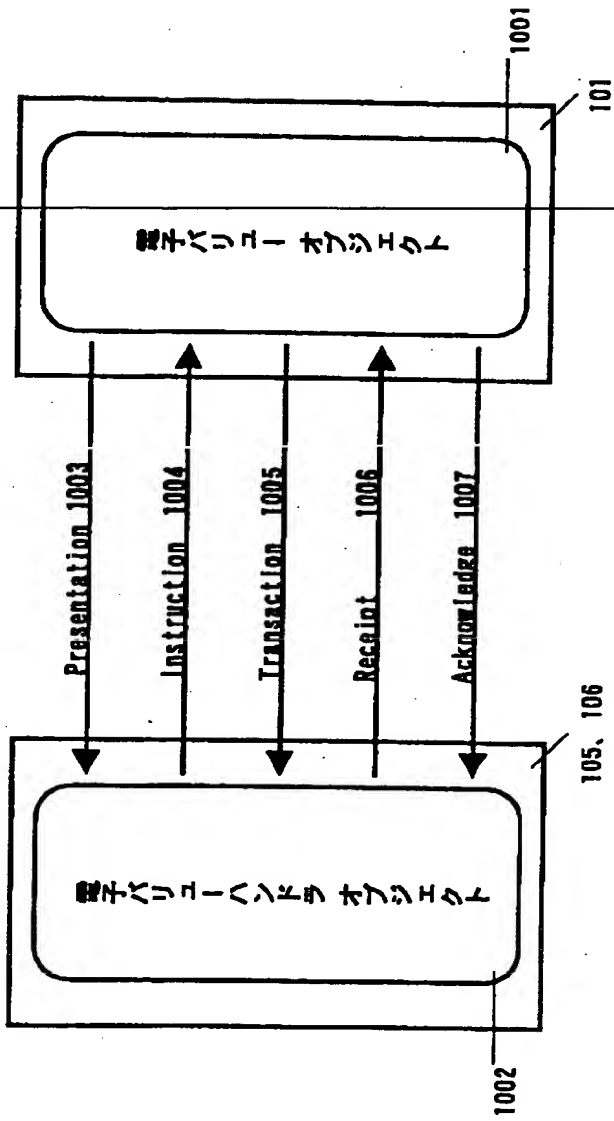
【図 8】



【図 9】

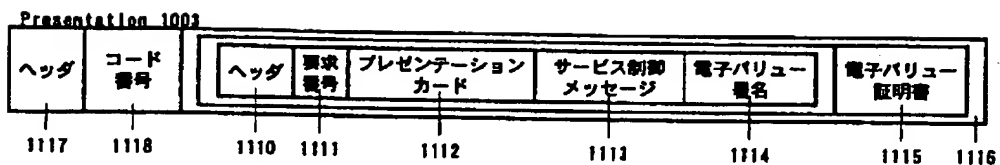


【図 1 0】



【図 11】

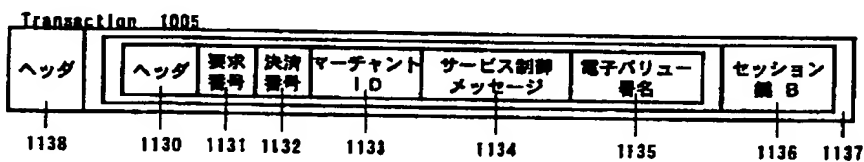
(a)



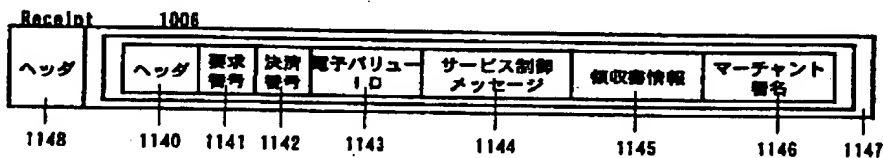
(b)



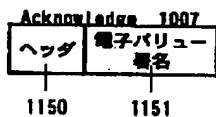
(c)



(d)



(e)



**EVML**



[illegible]

【图 14】

```
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
  <SC-module type="ticket" ID=1 number=$NUMBER start=$START_VALID end=$END_VALID
    used_flag=$USED validity_flag=$VALIDITY serial=$USE_SERIAL/>
  <SC-module type="verify_prop" ID=2 prop=$SEAT_NUM/>
  <SC-module type="set_message" ID=3 msg=$MESSAGE_2/>
</Description>
```

```
<Description about="SecurityInf" evID="10000000000000000000000000000001">
  <evOwner>
    <Description about="http://www.evalue.com/user/11000000000000000000000000000001"
      EntityName="Taro Suzuki"
      EntityID="11000000000000000000000000000001"/>
  </evOwner>
  <evResource>http://www.evalue.com/evalue/10000000000000000000000000000001</evResource>
  <evCertificate>
    0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
  </evCertificate>
  <evPrivateKey>0123456789</evPrivateKey>
  <evAuthKey>0123456789ABCDEF</evAuthKey>
  <evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>
</Description>
```

【図 1 5】

```

<SignedDescription about="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl"
  evID="10000000000000000000000000000001">
  <OptimumRpCtrl>
    <Description about="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl_M01">
      <RpType>MOBILE 01</RpType>
      <RepresentationCtrlData>
        <CARD name="Main">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
            <Do type="ACCEPT">
              <Go HREF="wallet:///evTransact"/>
            </Do>
            <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
            <BR><CENTER><IMG SRC="wallet:///evResource label=MAIN_IMG"></CENTER>
            <BR><UL>Date:<evP>$DATE</evP>
            <BR>Stadium:<A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
            <BR>Seat:<A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
            <BR><A HREF="Detail">Details</A></UL>
          </BODY>
        </CARD>
        <CARD name="Detail">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
            <Do type="ACCEPT">
              <Go HREF="wallet:///evTransact"/>
            </Do>
            <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
            <BR><UL>Date:<evP>$DATE</evP>
            <BR>Open Gate:<evP>$GATE_OPEN</evP>
            <BR>Stadium:<A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
            <BR><A HREF="wallet:///evResource label=MAP">Map</A>
            <BR>Seat:<A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
            <BR>Term of Validity: <evV>$START_VALID</evV> - <evV>$END_VALID</evV>
            <BR>Sponsor:<A HREF=<evP>$SPONSOR_URI</evP>><evP>$SPONSOR_NAME</evP></A>
            <BR>Contact:<A HREF="telephone:///dial num=<evP>$CONTACT_TELNUM</evP>">
              <evP>$CONTACT_TELNUM</evP></A>
            <BR>Issuer:<A HREF=<evP>$ISSUER_URI</evP>><evP>$ISSUER_NAME</evP></A>
            <BR><evP>$MESSAGE_1</evP>
            <BR><evV>$MESSAGE_2</evV>
            <BR><A HREF="Main">Top Page</A></UL>
          </BODY>
        </CARD>
      </RepresentationCtrlData>
    </Description>
  </OptimumRpCtrl>
  <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com"/>
  <Signature>3456789ABC</Signature>
</SignedDescription>

```



マーチャントオプション 805

【図 1 9】

a)

```
<SC-MSG>
  <scm_msg ID=1 number=1 start="1999.07.23T00:00+0900" end="2002.06.30T23:59+0900"
    used_flag=0 validity_flag=1 serial=0/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg="/>
</SC-MSG>
```

b)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630"/>
</SC-MSG>
```

c)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630"/>
</SC-MSG>
```

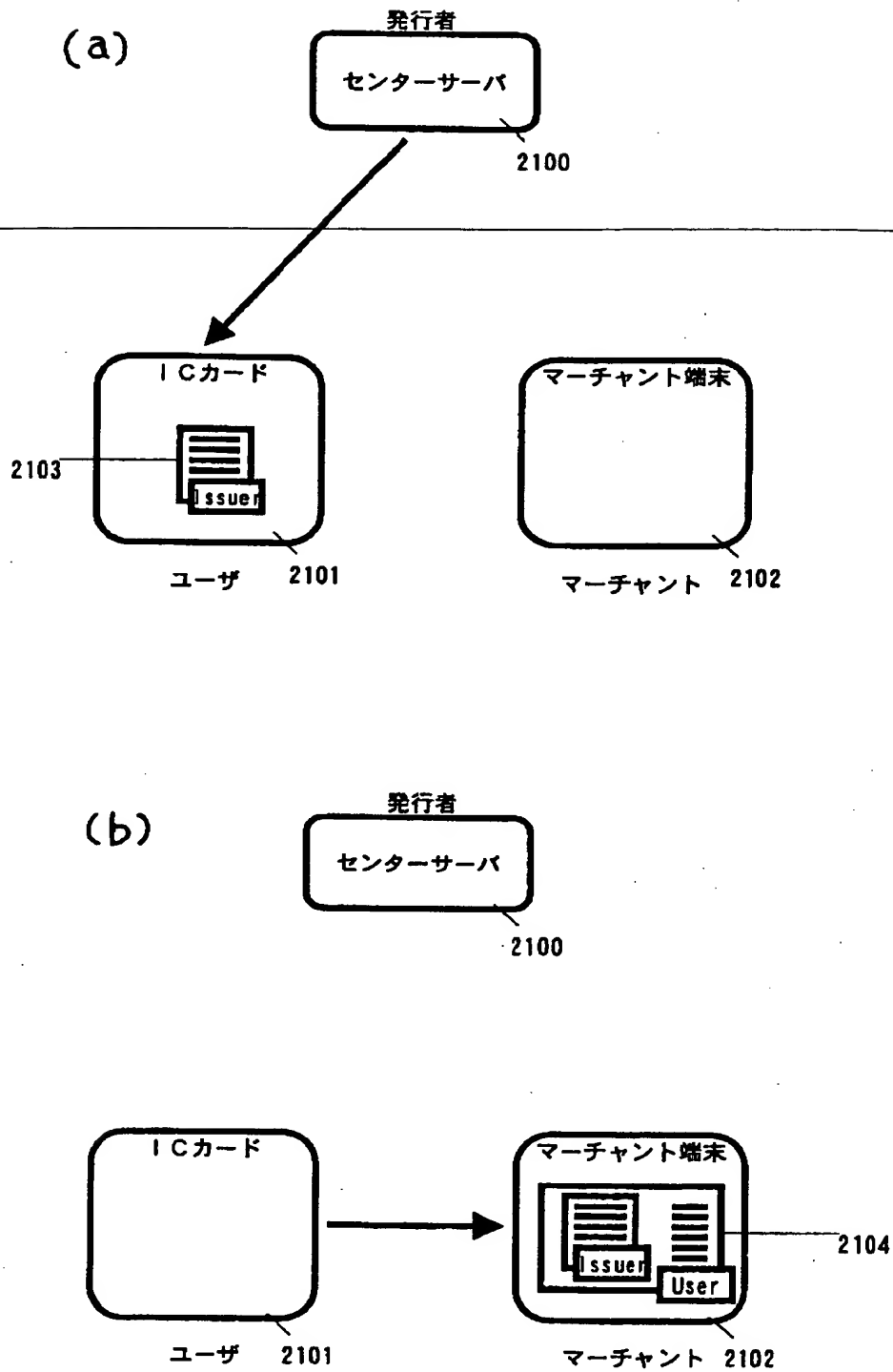
d)

```
<SC-MSG>
  <scm_msg ID=1 serial=1/>
</SC-MSG>
```

【図 2 0】

```
<SignedDescription about="ViableProperty" evID="10000000000000000000000000000001">
  <evFlag VALIDITY=1 USED=1/>
  <evProp name="USE_SERIAL" value=1/>
  <evProp name="NUMBER" value=0/>
  <evProp name="START_VALID" value="2002.06.30T12:25+0900"/>
  <evProp name="END_VALID" value="2002.06.30T23:59+0900"/>
  <evProp name="MESSAGE_2" value="Special News available: http://www.yis.co.jp/news/20020630"/>
  <SignedTime>2002.06.30T12:25+0900</SignedTime>
  <Signer rdf:resource="http://www.evaluate.com/evaluate/10000000000000000000000000000001"/>
  <Signature>A12345678A</Signature>
</SignedDescription>
```

【図 21】



【書類名】 要約書

【要約】

【課題】 匿名性と安全性、および利便性に優れ、価値情報の効率的な電子化と、各種の電子化された価値情報をユーザが効率的に取り扱うことが出来る電子財布を提供することを目的とする。

~~【解決手段】 電子バリューの固定属性を示すプレゼンテーションカード 8 0~~

1 は、サービス提供者によりデジタル署名されており、可変属性 8 0 2 は、この電子バリューの秘密鍵によってデジタル署名されている。また、サービス制御部 8 0 3 とセキュリティ情報部 8 0 4 と表示制御部 8 0 5 と表示リソース部 8 0 6 は、サービス提供者によりデジタル署名されている。これらのデジタル署名は、電子バリューオブジェクトが生成される度に検証される。

【選択図】 図 8



出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

---

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社

**THIS PAGE BLANK (USPTO)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**